Prüfer domain

Thierry Coquand

August 2008
A valuation domain is an integral domain $R$ such that for any $u, v$ in $R$ either $v$ divides $u$ or $u$ divides $v$.

Another formulation is that for any $s \neq 0$ in the field of fraction of $R$ we have $s$ in $R$ or $1/s$ in $R$.

**Theorem:** A valuation domain is integrally closed.

Indeed assume $s \neq 0$ is integral over $R$. We have an equation

$$s^n + a_1 s^{n-1} + \cdots + a_0 = 0$$

Then either $s$ is in $R$ (and we have finished) or $1/s$ is in $R$. But we have $s = a_1 + a_2 / s + \cdots + a_0 / s^{n-1}$ and hence $s$ is in $R$. 
Classically a Prüfer domain $R$ is a domain $R$ such that for any prime $p$ of $R$ the localisation $R_p$ is a valuation domain.

This means that for any $u, v \neq 0$ in $R$ then we have $v/u$ in $R_p$ or $u/v$ in $R_p$.

How to write this in a finite way (without points)?

We remark that if we have $v/u$ in $R_p$ then there exists $a$ in $R$ such that $p$ is in $D(a)$ and $v/u$ is in $R[1/a]$. 
Hence for any $u, v$ and any $p$ there exists $a$ such that $p$ is in $D(a)$ and $v/u$ is in $R[1/a]$ or $u/v$ is in $R[1/a]$.

By compactness of the Zariski spectrum we have finitely many elements $a_1, \ldots, a_n$ in $R$ such that $1 = D(a_1, \ldots, a_n)$ and for each $i$, we have $u/v$ is in $R[1/a_i]$ or $v/u$ is in $R[1/a_i]$.

This is a finite condition but we can simplify it a little

We can first assume $\sum a_i = 1$. Then taking $b$ to be the sum of all $a_i$ such that $u/v$ is in $R[1/a_i]$ we see that $u/v$ is in $R[1/b]$ and $v/u$ is in $R[1/1 - b]$.

We have used the fact that if $u_1/v_1 = u_2/v_2$ then $u_1/v_1 = u_2/v_2 = u_1 + u_2/v_1 + v_2$.
Thus we get the point-free condition: for any $u, v$ we can find $b$ such that $u/v$ is in $R[1/b]$ and $v/u$ is in $R[1/1 - b]$

This means $u/v = p/b^N$ and $v/u = q/(1 - b)^N$ for some $N$

Since $1 = D(b^N, (1 - b)^N)$ we can still simplify this to $u/v = d/c$ and $v/u = e/1 - c$

This gives the other equivalent condition: for any $u, v$ there exists $c, d, e$ such that $uc = vd$ and $v(1 - c) = eu$

Notice that this is a simple first-order (and even coherent) condition

A ring satisfying this condition is called *arithmetical*
Let $R$ be a Prüfer domain

We know that, locally, $R$ is a valuation domain

We know also that a valuation domain is integrally closed

Hence we deduce from a local-global principle that $R$ is integrally closed

We can follow this reasoning and get a direct proof that $R$ is integrally closed from the fact that $R$ is arithmetic (this is yet another illustration of the completeness of coherent logic)
Classically a Dedekind Domain can be defined to be a Noetherian Prüfer domain.

A Noetherian valuation domain is exactly a discrete valuation domain, which happens to be of Krull dimension $\leq 1$.

Hence (local-global property) a Dedekind domain is of Krull dimension $\leq 1$: a non zero prime ideal is maximal.

But several important properties of Dedekind domain hold already for Prüfer domain, which is a first-order notion (and which is not necessarily of dimension $\leq 1$).
A valuation domain is such that the divisibility relation is linear

Hence if we have finitely many elements $x_1, \ldots, x_n$ one of them divides all the other.

Over a Prüfer domain $R$ we deduce that we have $a_1, \ldots, a_n$ such that $1 = D(a_1, \ldots, a_n)$ and $x_i$ divides all $x_j$ in $R[1/a_i]$

As before we can simplify this condition by $1 = \sum a_i$ and there exists $b_{ij}$ such that $b_{ij} x_j = a_i x_i$
In this way we get the existence of a matrix $a_{ij}$ such that $1 = \sum a_{ii}$ and $a_{ij}x_j = a_{ii}x_i$

Such a matrix is called a principal localization matrix of the sequence $x_1, \ldots, x_n$

If all $x_i$ are $\neq 0$ we get $a_{ji}x_j = a_{jk}x_i$ and we have

$$<a_{1i}, \ldots, a_{ni}><x_1, \ldots, x_n> = <x_i>$$

In particular we have an inverse of the ideal $<x_1, \ldots, x_n>$ (the product is a non zero principal ideal)
Dedekind himself thought that the existence of such an inverse was *the* fundamental result about the ring of integers of an algebraic field of numbers (see J. Avigad’s historical paper on Dedekind)

Our argument is constructive, thus can be seen as an *algorithm* which computes this inverse over an arbitrary Prüfer domain

All we need is to know constructively

\[ \forall x \ y \exists u \ v \ w. \ xu = yv \land y(1 - u) = xw \]
Application

If $I \subseteq J$ are 2 f.g. ideals we can compute a f.g. ideal $K$ such that $J.K = I$

Indeed this is simple if $J$ is principal, and we can find $J'$ such that $J.J'$ is principal, and then $I.J' \subseteq J.J'$

In particular, if $I, J$ are f.g. ideals since we have $I.J \subseteq I + J$ we can find $K$ f.g. such that $I.J = (I + J).K$. It follows then that $K = I \cap J$

Hence: the intersection of two f.g. ideals is f.g. and we have an algorithm to find the generators of this intersection
This can be stated as: *any Prüfer Domain is coherent*

Classically one works with Dedekind Domain, that are Noetherian, and this remarkable fact is usually not stressed (Noetherian implies coherent in a trivial way)
The center map for a Prüfer Domain

**Theorem:** If $R$ is a Prüfer Domain then the center map $\psi : \text{Zar}(R) \rightarrow \text{Val}(R)$ is an isomorphism.

We show that $\psi$ is surjective.

We consider $s = x/y$ with $x, y$ in $R$.

We have $u, v, w$ such that $ux = vy$ and $(1 - u)y = wx$.

We can then check that we have $V_R(x/y) = \psi(D(u, w))$ and $V_R(y/x) = \psi(D(1 - u, v))$. 
It may be that $\psi$ is surjective but $R$ is not a Prüfer Domain.

An example is $R = \mathbb{Q}[x, y]$ with $y^2 = x^3$ which is not integrally closed.

**Proposition:** If $R$ is integrally closed and the center map is surjective then $R$ is a Prüfer Domain.
We present now a simple sufficient condition for $R$ to be a Prüfer domain

For any non zero $s$ in the field of fraction of $R$ we have to find $u, v, w$ in $R$ such that $u = vs$ and $(1 - u)s = w$

**Theorem:** If $s$ is a zero of a primitive polynomial in $R[X]$ then we can find $u, v, w$ integral over $R$ such that $u = vs$ and $(1 - u)s = w$

This is a fundamental result for producing integral elements
Prüfer domain

**Gilmer-Hoffmann’s Theorem**

We write $a_n s^n + \cdots + a_0 = 0$ with $a_n, \ldots, a_0$ in $R$ such that $1 = D(a_n, \ldots, a_0)$

We define

$$b_n = a_n, \quad b_{n-1} = b_n s + a_{n-1}, \quad \ldots, \quad b_1 = b_2 s + a_1$$

We then check that $b_n, b_n s, \ldots, b_1, b_1 s$ are all integral over $R$

We consider the ring $S = R[b_n, b_n s, \ldots, b_1, b_1 s]$. In this ring we have $1 = D(b_n, b_n s, \ldots, b_1, b_1 s)$ and we have $s$ in $S[1/b_i]$ and $1/s$ in $S[1/b_i s]$

Hence we can find $u, v, w$ in $S$ such that $u = vs$ and $(1 - u)s = w$
Applications

**Theorem:** If $S$ is the integral closure of a Bezout Domain $R$ in a field extension of its field of fractions then $S$ is a Prüfer Domain

Indeed if $s$ is in the field of fractions of $S$ then $s$ satisfies a polynomial equation $a_n s^n + \cdots + a_0 = 0$ with $a_n, \ldots, a_0$ in $R$ such that $1 = D(a_n, \ldots, a_0)$, since $R$ is a Bezout Domain

Two particular important cases are $R = \mathbb{Z}$ (algebraic integers) and $R = k[X]$ (algebraic curves)
Applications

**Proposition:** If $R$ is a Prüfer Domain and $s$ is in the field of fraction of $R$ then there exists $u, w$ in $R$ such that $R[s] = R[1/u] \cap R[1/w]$. In particular $R[s]$ is integrally closed, and hence, by the Gilmer-Hoffmann’s Theorem, $R[s]$ is a Prüfer Domain.

Indeed the equality $R[s] = R[1/u] \cap R[1/w]$ follows from $us = v$, $1 - u = ws$. 
We apply our results to the case of algebraic curves: we consider an algebraic extension $L$ of a field of rational functions $k(x)$.

If $a$ is an element of $L$ we have an algebraic relation $P(a, x) = 0$.

If $x$ does not appear in this relation then $a$ is algebraic over $k$: it is a constant of $L$. We let $k_0$ be the field of constants of $L$.

If $x$ appears, then $x$ is algebraic over $k(a)$ and $a$ is a parameter and then $L$ is algebraic over $k(a)$. We write $E(x_1, \ldots, x_n)$ the elements integral over $k[x_1, \ldots, x_n]$.
Algebraic curves

We consider the formal space \( X = \text{Val}(L, k) \)

Over \( X \) we define a sheaf of rings: if \( U \) is a non zero element of \( \text{Val}(L, k) \) it is a disjunction of elements of the form \( V(a_1) \land \cdots \land V(a_n) \).

We define \( \mathcal{O}_X(U) \) to be the set of elements \( f \) in \( L \) such that \( U \leq V(f) \) in \( \text{Val}(L, k) \).
Intuitively any $f$ in $L$ is a meromorphic function on the abstract Riemann surface $X$ and $U \subseteq V(f)$ means that $f$ is holomorphic over the open $U$

In particular we have $\Gamma(X, \mathcal{O}_X) = k_0$

This is an algebraic counterpart of the fact that the global holomorphic functions on a Riemann surface are the constant functions
Algebraic curves

If $p$ is a parameter and $b$ is in $E(p)$ then we have $E(p, 1/b) = E(p)[1/b]$.

More generally

$$\Gamma(V(p) \wedge V(1/b_1, \ldots, 1/b_m)) = E(p)[1/b_1] \wedge \cdots \wedge E(p)[1/b_m]$$
Since $E(p)$ is the integral closure of the Bezout Domain $k[p]$ we have that $E(p)$ is a Prüfer Domain.

Hence the sublattice $\downarrow V(p)$ of $\text{Val}(L, k)$ is isomorphic, via the center map, to $\text{Zar}(E(p))$.

The sheaf $\mathcal{O}_X$ restricted to the basic open $V(p)$ is isomorphic to the affine scheme $\text{Zar}(E(p))$, $\mathcal{O}$.
Algebraic curves as schemes

The pair $X, \mathcal{O}_X$ is thus a most natural example of a scheme, which is the glueing of two affine schemes.

For any parameter $p$ the space $X$ is the union of the two basic open $U_0 = V(p)$ and $U_1 = V(1/p)$.

$U_0$ is isomorphic to $\operatorname{Zar}(E(p))$.

$U_1$ is isomorphic to $\operatorname{Zar}(E(1/p))$.

The sheaf $\mathcal{O}_X$ restricts to the structure sheaf over each open $U_i$. 
The Genus of an Algebraic Curve

Following the usual cohomological argument, one can show

**Theorem:** The \( k_0 \)-vector space \( H^1(p) = E(p, 1/p)/(E(p) + E(1/p)) \) is independent of the parameter \( p \) and hence defines an invariant \( H^1(X, \mathcal{O}_X) \) of the extension \( L/k \).

In particular for \( L \) defined by \( y^2 = 1 - x^4 \) we find \( H^1(x) = \mathbb{Q} \)

For \( L = \mathbb{Q}(t) \) we find \( H^1(t) = 0 \)